Pwnie Express User Manual

Mobile product line

Pwn Pad 2014

(http://pwnieexpress.com/products/pwnpad)

The latest version of this manual is maintained here:
http://www.pwnieexpress.com/pages/documentation

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

Table of Contents:

- Legal disclaimers
- Getting started
  - Things to be aware of
  - Basic navigation
  - Connecting to wifi networks
  - Connecting USB devices
  - Recommended apps from Google Play
- Command terminals
  - Local terminal emulator
  - Remote terminal via SSH
  - Tethered terminal via USB cable
- One-touch pentesting
- Additional command-line pentesting tools
- Using the reverse shells
  - Reverse shell overview
  - Typical deployment overview
  - Activating the reverse shells
  - Configuring Backtrack to receive the reverse shells
  - Connecting to the reverse shells
  - Deploying to target network
- Maintaining your Pwnie device
  - Updating device software
  - Transferring files to/from your device
    - Transferring files via USB drive
    - Transferring files via ADB commands
    - Transferring files via SCP
- How to get support

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

Legal disclaimers

- All Pwnie Express products are for legally authorized uses only. By using this product you agree to the terms of the Rapid Focus Security, Inc. EULA: (http://pwnieexpress.com/pdfs/RFSEULA.pdf)

- This product contains both open source and proprietary software: Proprietary software is distributed under the terms of the Rapid Focus Security, Inc. EULA: (http://pwnieexpress.com/pdfs/RFSEULA.pdf). Open source software is distributed under one or more of the following licenses:

    - GNU PUBLIC LICENSE (HTTP://WWW.GNU.ORG/LICENSES/GPL.HTML).
    - BSD-3-CLAUSE LICENSE (HTTP://WWW.OPENSOURCE.ORG/LICENSES/BSD-3-CLAUSE):
    - OPENSSL TOOLKIT DUAL LICENSE (HTTP://WWW.OPENSSL.ORG/SOURCE/LICENSE.HTML)
    - APACHE LICENSE, VERSION 2.0 (HTTP://WWW.APACHE.ORG/LICENSES/LICENSE-2.0.HTML)

- As with any software application, any downloads/transfers of this software are subject to export controls under the U.S. Commerce Department's Export Administration Regulations (EAR). By using this software you certify your complete understanding of and compliance with these regulations.

Getting started

Things to be aware of

- The Pwnie Express mobile product line is designed exclusively for conducting network security assessments. As such, using these products as personal mobile devices is not recommended or supported.
- All “one-touch pentesting” apps should be closed “gracefully” with CTRL+C, which can be executed by pressing the **volume down button** on the right hand side and the **C** button on the terminal keyboard.
- Only one directly-attached external USB device is supported at a time. To attach multiple external USB adapters at once, an externally-powered USB hub is recommended, though a non-powered hub may support up to two devices at a time depending on power draw.
- The tablet’s internal wireless and Bluetooth hardware does not support packet injection or monitor mode. The included external USB wireless/Bluetooth adapters are the only supported adapters offering packet injection and monitor mode at this time.
- For full functionality, be sure to install recommend apps from the Google Play Store (see section “Recommended apps from Google Play” below).

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

Basic navigation

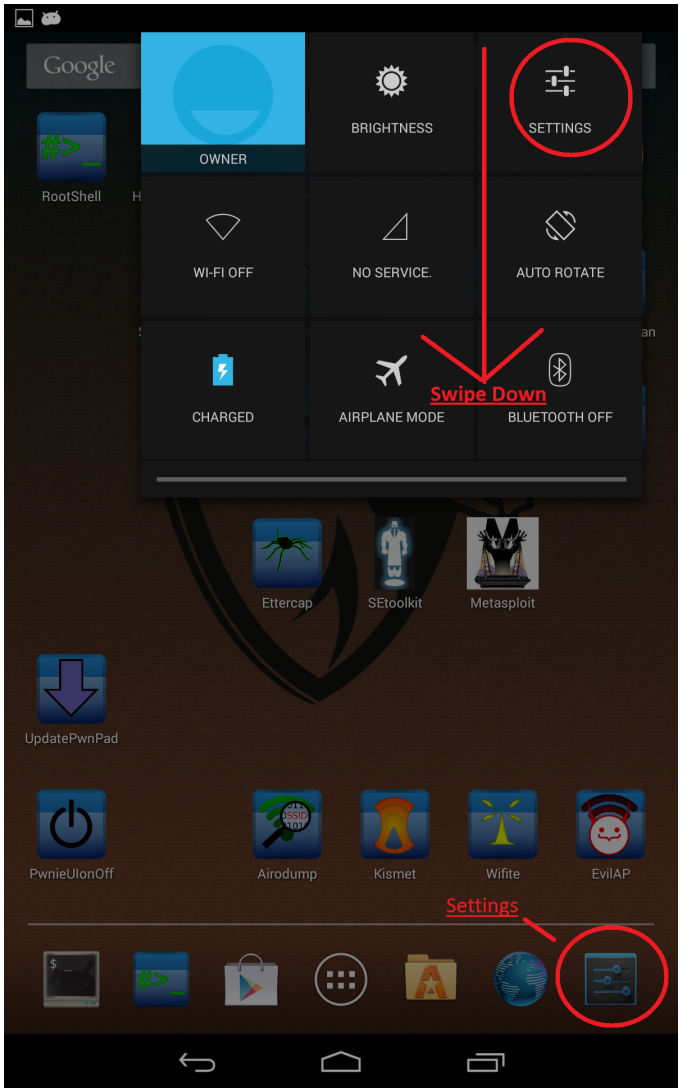
All basic tablet navigation uses the front-end Android operating system. Swiping, tapping, and tap-and-hold are all part of Android's native navigation system.

Switching between open apps: Simply swipe horizontally across the app / terminal window to switch to the next open app.

Closing apps: To close an app, tap the multi-view (double rectangle icon) in the bottom right hand corner. Then, from the app window list, swipe an app window off the screen and to the right to close the app. To verify an app has really stopped running, use the app manager within 'Settings > Apps > Running', tap 'Terminal Emulator', then tap 'Stop'. This will ensure the app has completely stopped. Below are a series of screenshots to illustrate this.

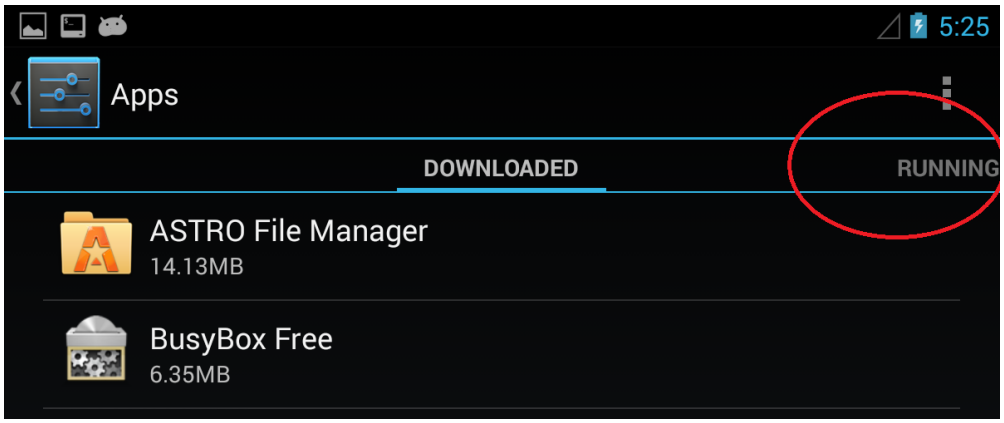
Typical open/close scenario when running Pwn Pad apps on desktop: (Example: Closing RootShell)

Keep the app manager open in the background to easily kill tasks by switching to multiview. To open app manager go to 'Settings > Apps > Running' (access settings icon in the tray on the bottom right or you can swipe from the top right side of the screen down):

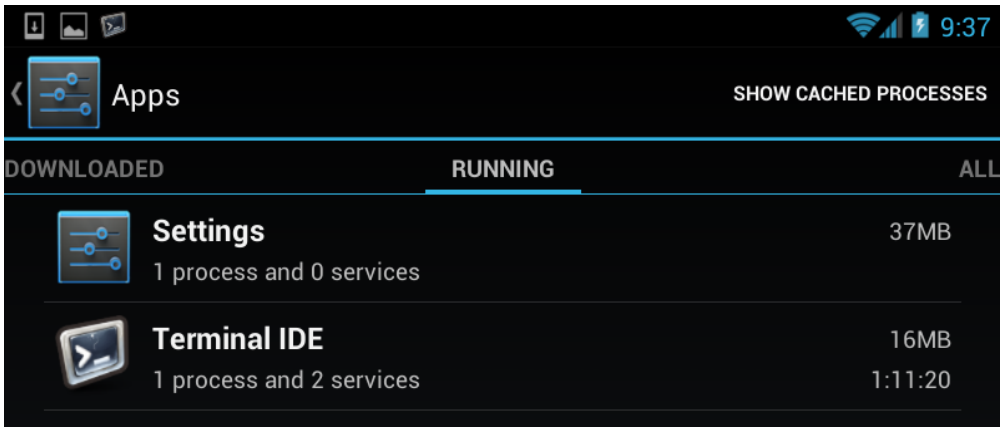


Next, go to 'Apps' then tap 'RUNNING' in the top right.

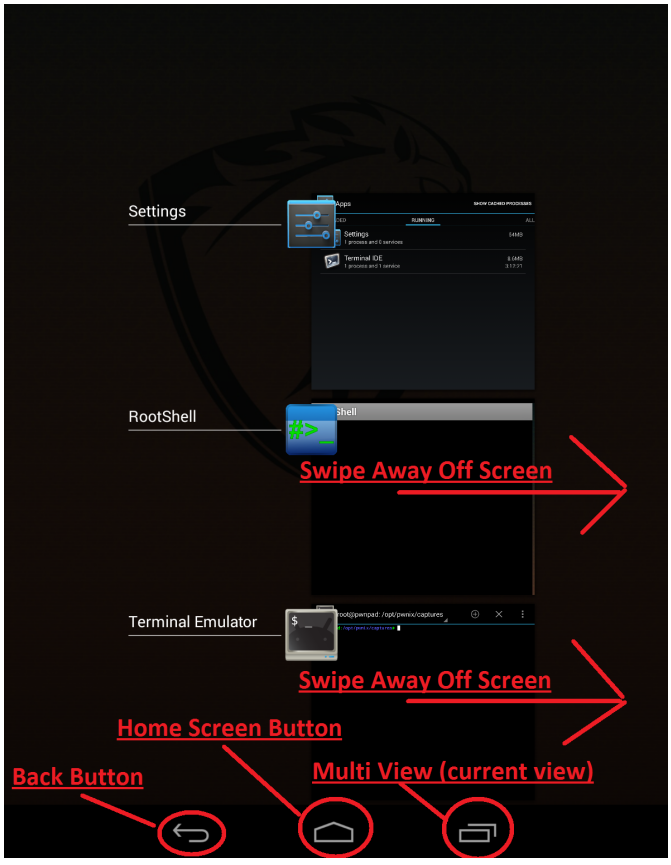
Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013



These are the only apps that need to be running:



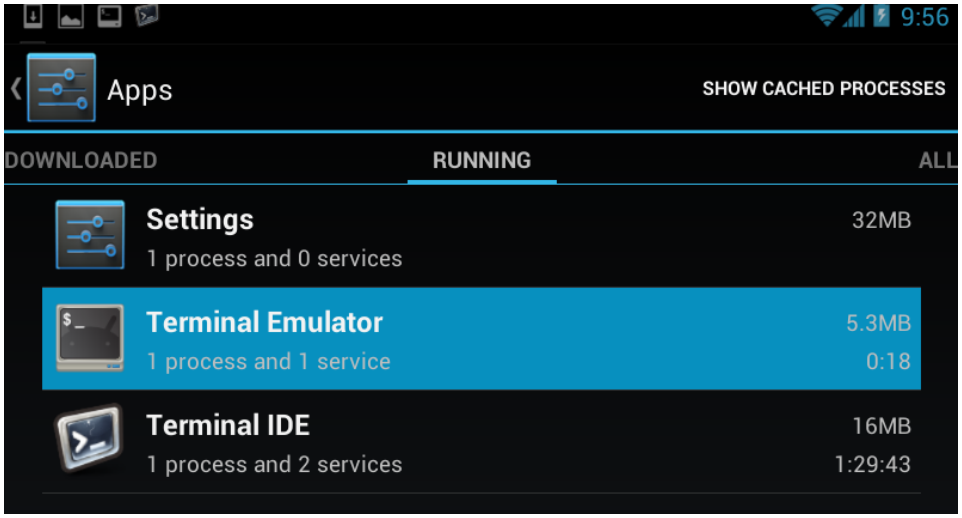
Select the ‘Home’ button (the house icon located in the center of the screen at the very bottom) to get back to the Pwn Pad desktop. Now select ‘RootShell’. To close ‘RootShell’ tap the multi-view icon in the bottom right hand corner (double rectangle icon):

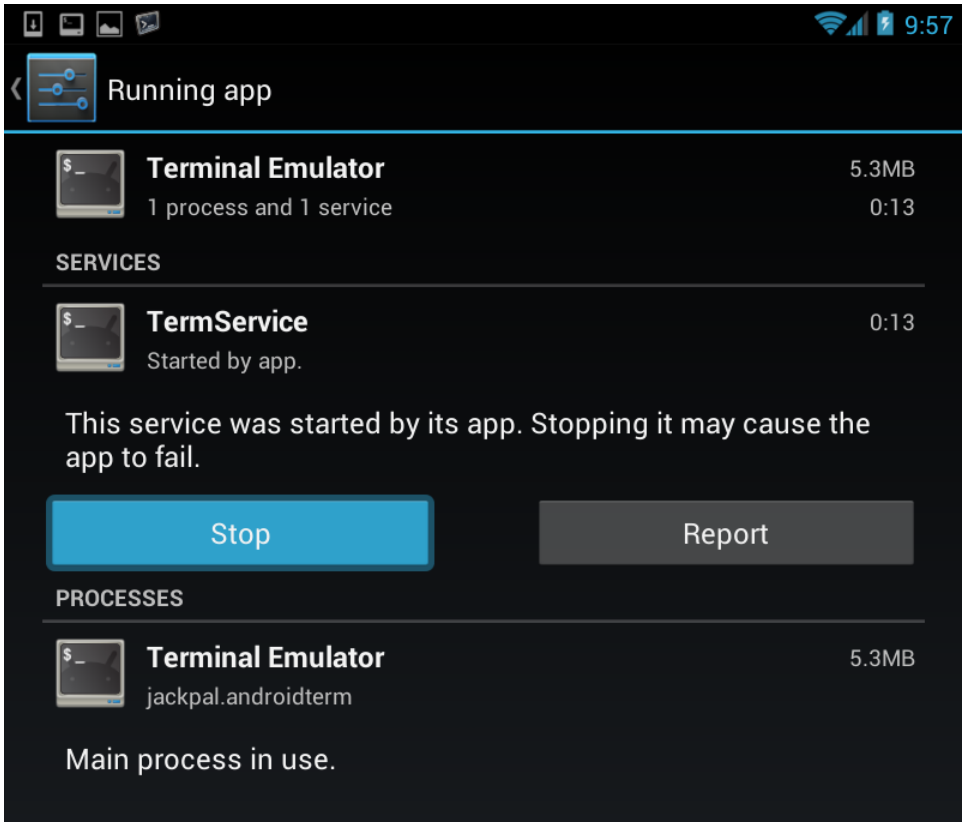


Every app will spawn both the app name and the Terminal Emulator. Swipe Terminal Emulator and the app name off the

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

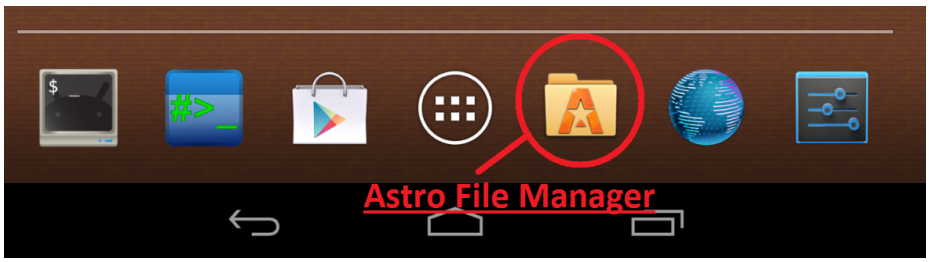
screen to close initially. Then tap the settings window showing ‘Running apps’ to kill the Terminal Emulator process completely:





Multi-view can also be very useful for switching between app (equivalent to ALT+TAB on a desktop/laptop computer).

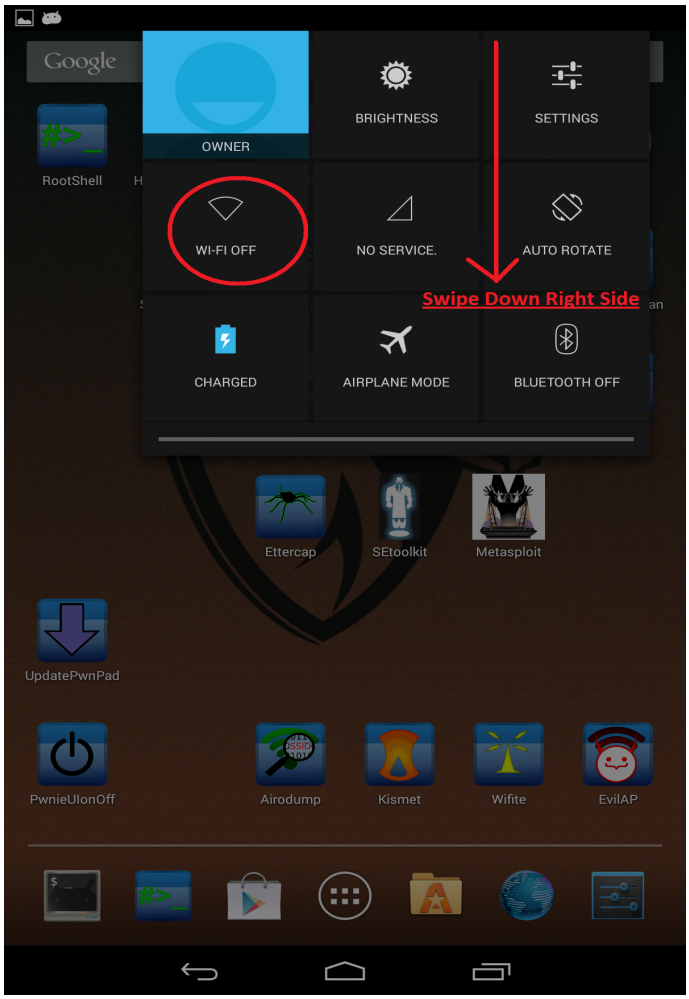
To browse local files through the GUI, open the ‘Astro File Manager’ app (must be installed via Google Play Store):

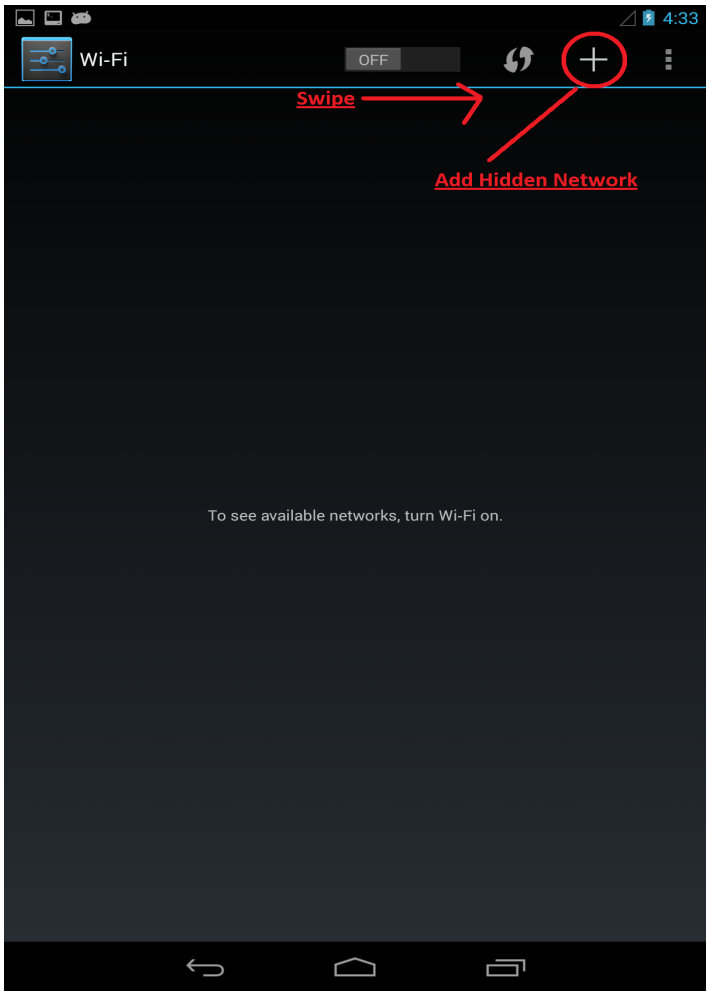


Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

Connecting to wifi networks

Swipe down from top right of the screen, select ‘WI-FI OFF’ , swipe Wi-Fi switch from OFF to ON. Select network to connect to below, type in network name and password and tap ‘connect’. For hidden networks tap the + button in the upper right hand corner and type in network name and select security type to enter password, tap ‘save’.





Connecting USB devices

How to connect OTG cable and included accessories:

Any USB accessories included with the Pwn Pad can be connected to the device via the provided OTG cable and attached via velcro to the back of the case. Each app that corresponds to the attached device will set up the device for you.

Included USB adapters will show up as the following interfaces in the Kali chroot environment:

TP-Link Wireless adapter - **wlan1**

Sena Bluetooth adapter - **hci0**

USB-Ethernet adapter - **eth0**

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

How to connect USB flash drives:

1. Connect a USB flash drive to the Pwn Pad via OTG cable.
2. Once connected, ‘ USB OTG Helper’ will appear, tap ‘OK’
3. Once ‘USB OTG Helper’ has loaded, select ‘MOUNT’
4. Once mounted, USB drive will show up under /storage/UsbOtgDrives/drive1/
5. Access from command line or ‘Astro File Manager’
6. To unmount safely open ‘USB OTG Helper’ and select ‘UNMOUNT’

   NOTE: USB drives can be accessed through Astro File Manager by going to ‘UsbOtgDrives’ once properly mounted. The folder ‘UsbOtgDrives’ will appear in ‘Storage’ within Astro File Manager.

Recommended apps from Google Play

For added functionality, we recommend downloading these additional Android apps from the Google Play store. While these apps are free, they are released under third-party licensing (as such, we are not able to bundle them into the product).

Note: A Google / Gmail account is required to access the Google Play Store.

- Astro file manager
- USB OTG helper
- Google Chrome or Firefox
- Fing

Command terminals

Local terminal emulator

Android Terminal Emulator is the local terminal application, used by one-touch pentesting apps to open a root shell into the Kali Linux chroot environment and run Pwn Pad scripts.

Each time a one-touch pentesting app is launched it will open Android Terminal Emulator, spawn a shell in the Kali chroot environment, then run the script for that tool.

To open a root shell within the Kali chroot environment, simply touch the ‘RootShell’ icon on the home screen. The root shell will start in the /opt/pwnix/captures/ directory.

Remote terminal via SSH

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

PwnieUIonOff

The Pwn Pad SSH server can be enabled using the 'PwnieUIonOff' icon on the home screen. **Note:** This will also enable the local Pwnie web UI. To start the SSH server only (without starting the Pwnie web UI), open a root shell and type:

 # service ssh start

Once SSH server is started, you can SSH into the Pwn Pad from a Linux/Mac computer on the same network, as shown:

user@linux/mac_computer$ **ssh pwnie@*ip_address_of_pwnpad***

The default "pwnie" user password is: pwnplug8000. Be sure to change this default password by running the following command after first logging in:

$ passwd

The "pwnie" user account is a standard user with sudo privileges. Most of the system commands and pentesting tools referenced in this manual must be run as root, as indicated by a hash tag (#) proceeding a command. Once logged in as "pwnie", you can sudo to root as follows:

$ sudo su -

Tethered terminal via USB cable

USB debugging mode (enabled by default) allows direct command terminal access to your Pwn Pad from a Linux host computer over USB.

To proceed, "android-adb-tools" must be installed on your Linux host computer. To install android-adb-tools on an Ubuntu 12.04 system:

user@linuxcomputer# **sudo add-apt-repository ppa:nilarimogard/webupd8**
user@linuxcomputer# **sudo apt-get update**
user@linuxcomputer# **sudo apt-get install android-tools-adb**

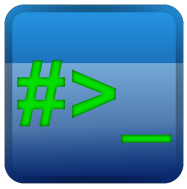
Once android-adb-tools is installed, attach the Pwn Pad to your Linux host computer via USB cable. Then, (on your Linux host computer) enter the following commands to access the Pwn Pad's Kali chroot environment:

user@linuxcomputer$ **adb shell**
shell@deb:/ $ **su**
root@deb:/ # **bootpwn**
root@pwnpad:/#

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

One-touch pentesting

Tip: The output of all one-touch pentesting apps is logged to /opt/pwnix/captures



RootShell

Provides Kali chroot environment access via Android Terminal Emulator.

HostMacChanger

Randomizes the hostname and MAC address of selected interface.

LogWiper

Securely wipes all captures, logs, tmp files, and/or bash history if desired.

StringsWatch

Be sure to connect the desired network adapter before running this app.
Shows human readable strings in the network traffic passing through the selected interface, with an option to log to /opt/pwnix/captures/stringswatch/

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

TCPdump

Be sure to connect the desired network adapter before running this app.
Displays raw network traffic on the selected interface, with an option to log to /opt/pwnix/captures/tcpdump/

Tshark

Be sure to connect the desired network adapter before running this app.
Displays network traffic via the command-line version of Wireshark, with an option to log to /opt/pwnix/captures/tshark/

Nmap

Be sure to connect the desired network adapter before running this app.
Runs an Nmap ping sweep (host discovery) on the selected interface, with an option to run service detection scan after the ping sweep completes. Scan output is saved to /opt/pwnix/captures/nmap_scans/

SSLstrip

Be sure to connect the desired network adapter before running this app.
“Strips” SSL encryption from certain connections by serving HTTP-only versions of requested URLS on the selected interface. Logs to /opt/pwnix/captures/passwords/

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

DNSspoof

The EvilAP app must be running before launching this tool.
Used in combination with EvilAP and Social Engineering Toolkit (website cloner), redirects all outbound DNS requests to the IP address of the local EvilAP (192.168.7.1).

Dsniff

Be sure to connect the desired network adapter before running this app.
Displays clear text usernames and passwords in transit on the selected interface, with an option to log to /opt/pwnix/captures/passwords/

Ettercap

Be sure to connect the desired network adapter before running this app.
Serves as a MITM tool suite to perform arp cache poisoning with known target IP addresses, with an option to log to /opt/pwnix/captures/ettercap/

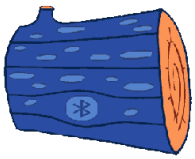
SEtoolkit

Launches the Social Engineering Toolkit, used for many MITM attacks combined with social engineering.

Metasploit

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

Launches the latest stable release of the Metasploit framework.



Bluelog

Be sure to connect the included USB SENA Bluetooth adapter before running this app.
Bluetooth scanning tool which logs device name, MAC address, and class id to /opt/pwnix/captures/bluetooth/

BluetoothScan

Be sure to connect the included USB SENA Bluetooth adapter before running this app.
Scans for Bluetooth devices using 'hcitool -i hci0 scan --flush --class --info' showing detailed bluetooth data about each devices found, including device type, class, and services available. Logs to /opt/pwnix/captures/bluetooth/

Ubertooth

An Ubertooth adapter (NOT INCLUDED) is required for this app - http://ubertooth.sourceforge.net/
Captures full-packet Bluetooth traffic using the Ubertooth tool suite.

Airodump

Be sure to connect the included USB TP-LINK wireless adapter before running this app.
Displays all in-range wireless APs and client devices in real time, including probe requests from clients. Option to save captures to /opt/pwnix/captures/wireless/. **Note:** Always use the 'Volume Down' button and 'C' key to close this app gracefully before disconnecting the wireless adapter!

Copyright 2014 [Pwnie Express](). All rights reserved. Manual revision: 12.18.2013

Kismet

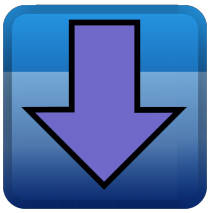
Be sure to connect the included USB TP-LINK wireless adapter before running this app.
Logs all in-range wireless devices and data traffic (packets). After launching, press “Tab”, then “Enter”, then press the “down arrow” in bottom left hand corner to minimize the on-screen keyboard. **Note:** Always use the ‘Volume Down’ button and ‘C’ key to close this app gracefully before disconnecting the wireless adapter!

Wifite

Be sure to connect the included USB TP-LINK wireless adapter before running this app.
Automated wireless attack / auditing tool providing front-end automation for the Aircrack-NG suite. After launching, select “1. wlan1” to place into the wireless adapter into monitor mode. Hit ‘Volume Down’ button and ‘C’ to select targets. **Note:** Always use the ‘Volume Down’ button and ‘C’ key to close this app gracefully before disconnecting the wireless adapter!

EvilAP

Be sure to connect the included USB TP-LINK wireless adapter before running this app.
Aggressive wireless access point used to forcefully associate wireless clients in range with using the client’s preferred network list. Select internet connection (wlan0 if connected to wifi), select channel, choose SSID network name to broadcast, enable probes or not. **Note:** Always use the ‘Volume Down’ button and ‘C’ key to close this app gracefully before disconnecting the wireless adapter!



UpdatePwnPad

Updates your Pwn Pad to the latest software release. Internet connection required. **Note:** The update process resets certain system config files in /etc and /opt/pwnix to their default state. If you have manually customized configuration files in these locations, be sure to back them up any before updating.

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

PwnieUIonOff

Enables/disables the local Pwnie web UI and SSH server (both are disabled by default). For the Pwn Pad, the Pwnie UI is primarily used for configuring reverse shells (see “Using the reverse shells”). The default username and password to access the UI or SSH server is: **pwnie : pwnplug8000**

Note: Be sure to change the “pwnie” user password before using your Pwn Pad in an untrusted environment. To do so, log into the device as the “pwnie” user via SSH, the run the following command:

$ passwd

Additional command-line pentesting tools

Thanks to the rock stars at the Kali Linux project (kali.org), all below pentesting tools are pre-installed as Debian packages and can be run from any path in the Kali chroot environment:

aircrack-ng	gpsd	p0f	sslstrip
amap	grabber	pingtunnel	stunnel
arp-scan	hping3	plecost	tcpflow
arping	httptunnel	proxychains	thc-ipv6
bed	hydra	proxytunnel	theharvester
bluelog	iodine	redfang	tinyproxy
bluez	john	scapy	ubertooth
cisco-auditing-tool	kismet	setoolkit	udptunnel
cisco-global-exploiter	lbd	sendEmail	ussp-push
cryptcat	mdk3	sipcrack	waffit
darkstat	metagoofil	sipsak	wapiti
dmitry	miranda	skipfish	weevely

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

dns2tcp	miredo	smtp-user-enum	wepbuster
dnsenum	nbtscan	snmpcheck	wifitap
dnstracer	netcat	socat	wifite
dsniff	netdiscover	sqlmap	xprobe2
ettercap	ngrep	sqlninja	
fierce	nikto	ssldump	
fimap	nmap	sslscan	
fping	onesixtyone	sslsniff	

Using the reverse shells

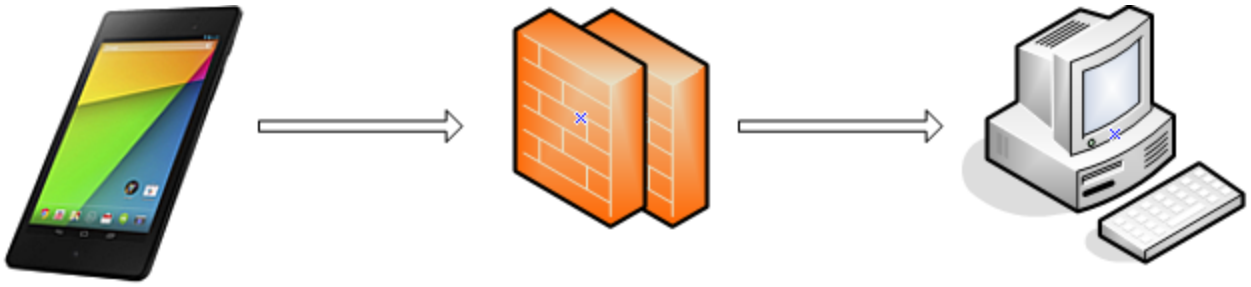
Reverse shell overview

- All Pwnie devices include aggressive reverse tunneling capabilities for persistent remote SSH access.
- SSH over HTTP, HTTPS/SSL, DNS, ICMP, and other covert tunneling options are available for traversing strict firewall rules, web filters, & application-aware IPS.
- All tunnels are encrypted via SSH and will maintain access wherever the device has an Internet connection - including wired, wireless, and 4G/GSM where available.

Typical deployment overview

1. On a staging/lab network, enable the desired reverse shells (see “Activating the reverse shells”)
2. Configure a Backtrack 5 system to receive the reverse shells (see “Configuring Backtrack to receive the reverse shells”)
3. Test the reverse shells in a lab / local LAN to confirm all shells are working as expected (see “Connecting to the reverse shells”)
4. Deploy the device to your target network and watch your SSH receiver for incoming shells (see “Deploying to target network”)

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013



Pwnie device on target network

Firewall on target network

SSH Receiver (Backtrack)

Activating the reverse shells

For Pwnie Express mobile products (Pwn Pad, etc.), the Pwnie UI is used for configuring the reverse shells.

1. To enable the Pwnie UI, touch the 'PwnieUIonOff' button on the home screen:

PwnieUIonOff

2. Open a web browser and access the Pwnie UI: https://*[device_ip_address]*:1443
3. The UI is SSL-enabled, but you will receive a warning as the certificate is self-signed.
4. At the login prompt, enter your username/password (default is **pwnie : pwnplug8000**)
5. The "Setup" page appears.

   Important: Be sure to change the default "pwnie" user password as soon as possible. This password can be changed in the Pwnie UI under "System Authentication". This will change the password for the 'pwnie' UI user and the 'pwnie' SSH user account.

6. Click "Reverse Shells" on the top menu.
7. Click the name of the shell you wish to configure.

   Tip: To best maintain persistent remote access, enable all of the reverse shells.

8. Enter the SSH shell receiver IP address or DNS name for each selected reverse shell. The device will connect to this shell receiver system to establish the reverse shell connections.
9. Choose how often the reverse shell connection should be attempted. By default, a shell connection will be attempted every minute (recommended).

   Tip: To use an HTTP proxy for the "SSH over HTTP Tunnel", enable the "Use HTTP Proxy" checkbox and enter the proxy server address and port (and optionally, proxy server credentials).

   Note: The HTTP proxy auth password is stored in clear text in /opt/pwnix/pwnix-scripts/script_configs

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

10. Click "Configure" to apply your changes for the reverse shell you're configuring.

    Note: The following SSH client config directives (/etc/ssh/ssh_config) are set on all devices to allow for automation of reverse shell connections. Be sure you understand the security implications of these settings before connecting to other SSH servers from the device.

    ```
    StrictHostKeyChecking no
    UserKnownHostsFile /dev/null
    ```

11. Proceed to configure Backtrack to receive the reverse shells.

Configuring Backtrack to receive the reverse shells

A Backtrack 5 system (Backtrack 5 R3 recommended) can serve as the SSH tunnel "receiver". Your Pwnie device will connect to this system when initiating the reverse shell connections.

Note: These steps assume you're using Backtrack 5 R3 as your SSH receiver. Older Backtrack distributions may be used, but different steps may apply.

1. Place your Pwnie device and the Backtrack system on the same local network/subnet
2. Login to the Backtrack system and open Firefox
3. Connect to the UI: https://*[device_ip_address]*:1443
4. Login to the UI when prompted.
5. Click "Reverse Shells" on the top menu.
6. Click the "Generate Backtrack config" link at the top of the page (under step 5) to download the "backtrack_receiver.sh" script.
7. Save the script file (backtrack_receiver.sh) into the root user's home directory (selected by default)
8. Open a terminal window and enter the following commands:

   # cd

   # chmod +x backtrack_receiver.sh

   # ./backtrack_receiver.sh

9. The script auto-configures and starts the reverse shell listeners on Backtrack.
10. When prompted, enter the desired certificate information for the stunnel SSL certificate (or just press ENTER to accept the defaults)
11. Once the auto-config script completes you will see:

    ```
    [+] Setup Complete.
    [+] Press ENTER to listen for incoming connections..
    ```

12. Press ENTER to watch for incoming device connections. Each reverse shell will attempt to connect using the interval you specified in the UI.

    Tip: You can list all active device connections at any time by typing:

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

 # netstat -lntup4 | grep 333

13. Proceed to “Connecting to the reverse shells”.

Connecting to the reverse shells

1. Open a terminal window on your Backtrack shell receiver system and connect to any available “listening” Pwnie device shell as follows:

    - **Standard SSH:** ssh pwnie@localhost -p 3333
    - **SSH Egress Buster:** ssh pwnie@localhost -p 3334
    - **SSH over DNS:** ssh pwnie@localhost -p 3335
    - **SSH over SSL:** ssh pwnie@localhost -p 3336
    - **SSH over 4G/GSM:** ssh pwnie@localhost -p 3337
    - **SSH over HTTP:** ssh pwnie@localhost -p 3338
    - **SSH over ICMP:** ssh pwnie@localhost -p 3339

1. Enter your Pwnie device’s “pwnie” user password and voila! You're now remotely connected to the device through the reverse shell.
2. Proceed to “Deploying to target network”

Standard SSH / SSH Egress Buster Note: If there’s no firewall between your Pwnie device and your shell receiver system, be sure the shell receiver system SSH server is listening on the ports you selected for the Standard Reverse SSH and SSH Egress Buster shells in the UI. For example, if you set port 31337 for Standard Reverse SSH, add the line “Port 31337” to /etc/ssh/sshd_config, then restart SSHd (/etc/init.d/ssh restart).

Tip: The SSH receiver address can be anonymized using the “Tor Hidden Service” feature as described here http://www.securitygeneration.com/security/reverse-ssh-over-tor-on-the-pwnie-express/

Special thanks to Sebastien J. of Security Generation for streamlining the SSH receiver setup process, and to Lance Honer for his resilient autossh script improvements.

Deploying to target network

1. Place your shell receiver system behind a public-facing firewall.
2. Configure the appropriate port forwarders on your firewall:

    - **Standard Reverse SSH:**
      Forward the port selected in the UI to port 22 of your shell receiver.

    - **SSH over HTTP:**
      Forward port 80 to port 80 of your shell receiver system

    - **SSH over SSL:**

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

Forward port 443 to port 443 of your shell receiver system

- **SSH over DNS:**
  Forward UDP port 53 to UDP port 53 of your shell receiver system

- **SSH over ICMP:**
  Requires your shell receiver system to be directly connected to the Internet (no firewall).

- **SSH over 3G:**
  Forward the port selected in the UI to port 22 of your shell receiver system

- **SSH Egress Buster:**
  Forward all ports selected in the UI to port 22 of your shell receiver system

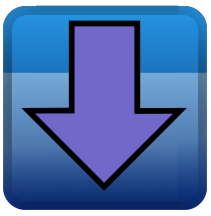
1. In the Pwnix UI (“Reverse Shells” page), configure the reverse shells to connect to your firewall’s public IP address (or DNS name if available).
2. You can now deploy your Pwnie device to your target network. The device will automatically “phone home” to your shell receiver system, providing encrypted remote access to your target network.

   Tip: In some environments you may wish to schedule a nightly reboot of the device to re-initiate all connections from the device side. This way, if some part of the connection process crashes on the device side (for example, sshd), the connection process will start “fresh” again after the reboot.

Maintaining your Pwnie device

Updating device software

To update your Pwn Pad to the latest software release, connect your Pwn Pad to the Internet, then press the “UpdatePwnPad” button on the home screen:



UpdatePwnPad

Note: The update process resets certain system config files in /etc and /opt/pwnix to their default state. If you have manually customized configuration files in these locations, be sure to back them up any before updating.

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

Transferring files to/from your device

Transferring files via USB drive

Note: The “USB-OTG Helper” and “Astro File Manager” apps must be installed before proceeding (see “Recommended apps from Google Play”).

1. Connect a USB flash drive to the Pwn Pad using the OTG cable.
2. If USB-OTG Helper pops up to manage the device, tap ‘OK’. If not, open USB-OTG Helper manually, then tap ‘Mount’. (If running for the first time, grant the app root access).
3. Open a root shell, and type the following:

   # cd ..
   # cp -a captures/ /sdcard/

4. Open ‘Astro File Manager’, select ‘sdcard0’ then tap and hold on ‘captures’ folder.
5. Select ‘copy’ in the bottom left hand corner.
6. Tap ‘storage’ in the top left hand corner, then tap the ‘UsbOtgDrives’ folder, then ‘drive1’, then ‘Paste’.
7. To delete the temporary captures folder in /sdcard/, tap ‘storage’ again, tap ‘sdcard0’ and tap and hold on the ‘captures’ folder, tap ‘delete’ in the bottom of the window.
8. Go back to USB-OTG Helper via the multiview button in the bottom right hand corner of the screen, or by opening USB-OTG Helper again.
9. Tap ‘UNMOUNT’ to safely remove the drive.

Transferring files via ADB commands

Note: These steps require ‘android-adb-tools’ to be installed on a Linux host computer:

1. Attach the Pwn Pad to your Linux computer with ADB tools installed.
2. Open a root shell on your Linux computer and change directory to the desired location to receive files to:

   user@linuxcomputer$ **mkdir captures**
   user@linuxcomputer$ **cd captures/**
   user@linuxcomputer$ **adb shell**
   shell@deb:/ $ **su**
   root@deb:/ # **bootpwn**
   root@pwnpad:/# **cd /opt/pwnix**
   root@pwnpad:/# **cp -a captures/ /sdcard/**
   root@pwnpad:/# **exit**
   root@deb:/ # **exit**
   shell@deb:/ $ **exit**
   user@linuxcomputer$/ **adb pull /sdcard/captures/**

3. To remove temporary captures folder from /sdcard:

   user@linuxcomputer$/ **adb shell**

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013

shell@deb:/ $ **su**
root@deb:/ # **rm -r /sdcard/captures/**

Note: This method will only pull folders with files in them, and not empty directories

Transferring files via SCP

Note: Using scp does not require having to copy the captures folder to /sdcard/.

1. Enable the Pwn Pad's local SSH server (see "Remote terminal via SSH").
2. From a Linux host computer connected to the same local network:

   user@linuxcomputer$ **scp -r pwnie@***ip_address_of_pwnpad***:/opt/pwnix/captures/ .**

How to get support

- Pwnie Express Support Portal: http://www.pwnieexpress.com/pages/support
- Pwnie Express Community Support Forum: http://forum.pwnieexpress.com

Copyright 2014 Pwnie Express. All rights reserved. Manual revision: 12.18.2013